

Amendments to the Drawings:

The attached sheets of drawings include changes to Figures 1 and 2a-2d. These sheets, which include Figs. 1 and 2a-2d, replace the original sheets including Figs. 1 and 2a-2d.

Attachment: Replacement Sheets

REMARKS

Claims 1-26 are presented for further examination. Claims 1-24 have been amended. Claims 25 and 26 are new.

In the Office Action mailed March 28, 2008, the Examiner objected to the drawings under 37 C.F.R. § 1.83(a) because they failed to show “MH12” and “MH21” as described in the specification on page 5, line 10, and page 6, line 1. Claims 1-5 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 6,094,487 (“Butler”). Claims 10, 15, and 20 were rejected as obvious over Butler in view of U.S. Patent Publication No. 2002/0090089 (“Branigan”). Claims 6-9 were rejected under 35 U.S.C. § 103(a) as obvious over Butler in view of U.S. Patent No. 6,853,729 (“Mizikovsky”). Claims 11-14, 16-19, and 21-24 were rejected as obvious over Butler in view of Mizikovsky and Branigan.

Applicant respectfully disagrees with the bases for the rejections and request reconsideration and further examination of the claims.

Amendments to Specification

Pages 1-3 of the specification have been amended to correct grammatical and typographical errors. No new matter has been added.

The specification on page 6, line 1 has been amended such that “MH21” and in other places “MH11” now read “MH12” for clarity and consistency.

Amendments to the Drawings

Applicant has amended Figure 1 as requested by the Examiner to now show “MH1,” “MH1,” and “cell” to be “MH12,” “MH13,” and “cell 1,” respectively. Figures 2a-2d have been amended wherein “MH21” now reads “MH12,” “conformation message” is now “confirmation message,” and in Figure 2c “return confirmation message” is moved to a correct position. Applicant respectfully requests that the Examiner approve and enter the substitute drawings accompanying this Amendment.

Claim Rejections

Applicant has amended claim 1 to further clarify the disclosed embodiments of the invention. No new matter has been introduced that goes beyond the scope of the original disclosure.

Claim 1 is directed to a method for distributing encryption keys in a Wireless Local Area Network (WLAN) that comprises receiving by an authentication device an authentication request containing identification information for identity authentication from a mobile host; authenticating the mobile host according to the identification information; if authentication fails, then sending an ACCESS_REJECT information to the mobile host, and if authentication succeeds then sending key-related information M1 to an access point (AP) and a message comprising ACCESS_ACCEPT information to the mobile host, wherein a key-related information M2 is comprised in the message comprising the ACCESS_ACCEPT information, the message including ACCESS_ACCEPT information that is encrypted, the key-related information M1 being used to obtain a key by the AP, the message comprising the ACCESS_ACCEPT information used to obtain the key by the mobile host.

Butler (U.S. Patent No. 6,094,487) is directed to an encryption key generation system that generates encryption keys at both an originating terminal and a terminating terminal of a wireless network. A central controller is disclosed that generates a shared secret based on the identification of a requesting terminal and a first number, which can be random. The central controller broadcasts the first number to all terminals. A second number is generated by the central controller incorporating the shared secret data and the terminating terminal's identification information. The requesting terminal generates the shared secret data using the first number and predetermined algorithms and generates an encryption key based on the first number and the shared secret data. The terminating terminal then decodes the shared secret data from the second number and generates the same encryption key using the first number and the shared secret data.

The inventors have reviewed the Butler reference and respectfully submit that none of the first number, the second number, the shared secret, and the first and second encryption keys described by Butler can be regarded as the "key-related information M1" as recited in amended claim 1. More specifically, the first number described by Butler is **broadcast periodically to the**

ISU's for authentication and the generation of shared secret data (see Butler, column 1, lines 58-60). In contrast, the key-related information M1 recited in amended claim 1 is sent to the access point (AP) when the authentication succeeds. In other words, the destinations and conditions for sending (or broadcasting) between the claimed method and that disclosed by Butler are completely different.

Accordingly, the first shared secret data (SSD) and the second SSD that are generated based on the first number in Butler (column 2, lines 7-13) are different from the key-related information M1 recited in claim 1. Furthermore, the second number generated based on the second SSD (see Butler, column 2, lines 14-15) and sent to the terminating ISU when the request is valid (see Butler, column 3, lines 53-54, and lines 60-61) is different from the key-related information M1 sent to the AP when the authentication succeeds, as recited in amended claim 1 submitted herewith.

In addition, the third SSD generated that is identical to the first SSD and generated based on the second number (see Butler, column 2, lines 17-19), are different from the key-related information M1 recited in claim 1. Also, the first and second encryption keys generated based on the first and third SSD and the first number in Butler are also different from the key-related information M1.

Although the Examiner asserts that the control center disclosed by Butler functions as both the authentication device and the AP, the inventors respectfully disagree that the control center can function as the AP because one skilled in the art will recognize that the functions of the authentication device and the AP are quite different in implementing the solution as recited in amended claim 1. Butler does not mention or suggest that the control center can function as the AP.

Specifically, according to the claimed solution and method recited in claim 1, the process of the encryption key distribution is combined with the access process of a mobile host. As known to those skilled in the art, the AP plays a different role in access to the mobile host from the authentication device. In addition, the AP as limited in amended claim 1 obtains the encryption key by using the key-related information M1. In contrast, Butler is completely silent about an access point (or any device) that can play a role in accessing the ISU to say nothing of how the AP obtains the encryption key.

In view of the foregoing, applicant respectfully submits that the control center as disclosed by Butler cannot be regarded as a combination of the authentication device and AP as recited in claim 1. Inasmuch as all of the rejections rely upon the primary reference Butler, which applicant has traversed as set forth above, applicant respectfully submits that Butler does not teach or suggest the method recited in claims 1-5, and the combination of Butler with Branigan does not obviate claims 10, 15, and 20, or with Mizikovsky does not obviate claims 6-9, or with Mizikovsky and Branigan obviate claims 11-14, 16-19, and 21-24. Thus, claims depending from claim 1, *i.e.*, claims 2-24, are allowable for the features recited therein as well as for the reasons why claim 1 is allowable.

New independent claims 25 and 26 correspond to the amended method claim 1 and are directed to an authentication device and a system, respectively. Applicants respectfully submit that these two new independent claims are allowable for the reasons discussed above with respect to independent claim 1.

In view of the foregoing, applicant respectfully submits that all of the claims remaining in this application are clearly in condition for allowance. In the event the Examiner finds minor informalities that can be resolved by telephone conference, applicant respectfully requests that the Examiner contact applicant's undersigned representative by telephone at (206) 622-4900 in order to expeditiously resolve prosecution of this application. Consequently, early and favorable action allowing these claims and passing this case to issuance is respectfully solicited.

Application No. 10/506,765
Reply to Office Action dated March 28, 2008

The Director is authorized to charge any additional fees due by way of this Amendment, or credit any overpayment, to our Deposit Account No. 19-1090.

Respectfully submitted,
SEED Intellectual Property Law Group PLLC

/E. Russell Tarleton/
E. Russell Tarleton
Registration No. 31,800

ERT:alb

Enclosure:

5 Sheets of Replacement Drawings (Figures 1 and 2a-2d)

701 Fifth Avenue, Suite 5400
Seattle, Washington 98104
Phone: (206) 622-4900
Fax: (206) 682-6031

1226283_1.DOC